Security Technical Operational Report

# Technical Operational (Local Generated)

# Technical Security Assessment Report

## Technical Summary [TECHNICAL\_SUMMARY\_PLACEHOLDER]

## Vulnerability Analysis

### Code Security Issues [CODE\_SECURITY\_PLACEHOLDER]

### Dependency Vulnerabilities [DEPENDENCY\_VULNERABILITIES\_PLACEHOLDER]

### Architecture Security Review [ARCHITECTURE\_REVIEW\_PLACEHOLDER]

## Detailed Technical Findings

### Critical Vulnerabilities [CRITICAL\_TECHNICAL\_FINDINGS\_PLACEHOLDER]

### High-Risk Issues [HIGH\_RISK\_TECHNICAL\_FINDINGS\_PLACEHOLDER]

### Medium-Risk Issues [MEDIUM\_RISK\_TECHNICAL\_FINDINGS\_PLACEHOLDER]

## Security Testing Results [SECURITY\_TESTING\_RESULTS\_PLACEHOLDER]

## Technical Recommendations [TECHNICAL\_RECOMMENDATIONS\_PLACEHOLDER]

## Implementation Guidelines [IMPLEMENTATION\_GUIDELINES\_PLACEHOLDER]

## Security Monitoring and Alerting [MONITORING\_RECOMMENDATIONS\_PLACEHOLDER]

## Executive Summary

No README found; executive summary is derived from scan findings and templates.

## Scan Summary

- Total findings: 15

- HIGH: 1

- MEDIUM: 5

- LOW: 3

- INFO: 6

## Detailed Findings and Analysis

### 1. Hardcoded Credentials (HARDCODED-SECRET)

- Severity: HIGH

- Location: app\auth.py:6

- Description: Sensitive credentials are hardcoded in the source code, making them accessible to anyone with code access.

\*\*Evidence (code snippet):\*\*

```

JWT\_SECRET = 'demo\_jwt\_secret'

```

- Recommendation: Refer to template remediation.

### 2. WEAK-CRYPTO-MD5 (WEAK-CRYPTO-MD5)

- Severity: MEDIUM

- Location: app\auth.py:0

\*\*Evidence (code snippet):\*\*

```

Use of MD5 detected

```

- Recommendation: Refer to template remediation.

### 3. INSECURE-TEMPFILE (INSECURE-TEMPFILE)

- Severity: LOW

- Location: app\file\_upload.py:9

\*\*Evidence (code snippet):\*\*

```

tmp = tempfile.NamedTemporaryFile(delete=False)

```

- Recommendation: Refer to template remediation.

### 4. POTENTIAL-XSS-TEMPLATE (POTENTIAL-XSS-TEMPLATE)

- Severity: MEDIUM

- Location: app\patient\_routes.py:2

\*\*Evidence (code snippet):\*\*

```

# Demonstrates PHI handling, render\_template\_string usage, and logging of PHI for analyzer evidence.

```

- Recommendation: Refer to template remediation.

### 5. POTENTIAL-XSS-TEMPLATE (POTENTIAL-XSS-TEMPLATE)

- Severity: MEDIUM

- Location: app\patient\_routes.py:4

\*\*Evidence (code snippet):\*\*

```

from flask import Blueprint, request, jsonify, render\_template\_string

```

- Recommendation: Refer to template remediation.

### 6. POTENTIAL-XSS-TEMPLATE (POTENTIAL-XSS-TEMPLATE)

- Severity: MEDIUM

- Location: app\patient\_routes.py:12

\*\*Evidence (code snippet):\*\*

```

return render\_template\_string(template)

```

- Recommendation: Refer to template remediation.

### 7. JS-DEPENDENCY-POTENTIAL-RISK (JS-DEPENDENCY-POTENTIAL-RISK)

- Severity: LOW

- Location: package.json:0

\*\*Evidence (code snippet):\*\*

```

express: ^4.18.2

```

- Recommendation: Refer to template remediation.

### 8. JS-DEPENDENCY-POTENTIAL-RISK (JS-DEPENDENCY-POTENTIAL-RISK)

- Severity: LOW

- Location: package.json:0

\*\*Evidence (code snippet):\*\*

```

lodash: ^4.17.21

```

- Recommendation: Refer to template remediation.

### 9. DEPENDENCY-VERSION-PIN (DEPENDENCY-VERSION-PIN)

- Severity: INFO

- Location: requirements.txt:1

\*\*Evidence (code snippet):\*\*

```

Flask pinned to 2.3.2

```

- Recommendation: Refer to template remediation.

### 10. DEPENDENCY-VERSION-PIN (DEPENDENCY-VERSION-PIN)

- Severity: INFO

- Location: requirements.txt:2

\*\*Evidence (code snippet):\*\*

```

PyJWT pinned to 2.8.0

```

- Recommendation: Refer to template remediation.

### 11. DEPENDENCY-VERSION-PIN (DEPENDENCY-VERSION-PIN)

- Severity: INFO

- Location: requirements.txt:3

\*\*Evidence (code snippet):\*\*

```

mysql-connector-python pinned to 8.1.0

```

- Recommendation: Refer to template remediation.

### 12. DEPENDENCY-VERSION-PIN (DEPENDENCY-VERSION-PIN)

- Severity: INFO

- Location: requirements.txt:4

\*\*Evidence (code snippet):\*\*

```

PyYAML pinned to 6.0

```

- Recommendation: Refer to template remediation.

### 13. DEPENDENCY-VERSION-PIN (DEPENDENCY-VERSION-PIN)

- Severity: INFO

- Location: requirements.txt:5

\*\*Evidence (code snippet):\*\*

```

paramiko pinned to 2.12.0

```

- Recommendation: Refer to template remediation.

### 14. DEPENDENCY-VERSION-PIN (DEPENDENCY-VERSION-PIN)

- Severity: INFO

- Location: requirements.txt:6

\*\*Evidence (code snippet):\*\*

```

pycrypto pinned to 2.6.1

```

- Recommendation: Refer to template remediation.

### 15. DEPENDENCY-POTENTIALLY-RISKY (DEPENDENCY-POTENTIALLY-RISKY)

- Severity: MEDIUM

- Location: requirements.txt:6

\*\*Evidence (code snippet):\*\*

```

pycrypto==2.6.1

```

- Recommendation: Refer to template remediation.

## Repository Policies (excerpts)

### policies\access\_control\_policy.md

# Access Control Policy (Mocked)

Describes roles, MFA requirements, password rules, and privileged access review cadence. Useful for enriching access-control related findings.

### policies\breach\_response\_policy.md

# Breach Response Policy (Mocked)

Provides detection, escalation, notification timelines and forensic steps. Useful for report generation that includes incident response guidance.

### policies\privacy\_policy.md

# MedSecure Hospital Privacy Policy (Mocked)

This mocked privacy policy describes PHI handling, retention, third-party sharing, and patient rights. Use this file to provide context for compliance report generation.

- Data types: demographics, MRN, clinical notes, imaging, billing  
- Retention: active records while in care, 7 years post-treatment for inactive  
- Third-party sharing: BAAs required  
- Contact: privacy@medsecure-hospital.example

## Methodology

Automated scanners used:

- CodeT5-based static heuristics (pattern checks)

- SCA heuristics scanning requirements.txt and package.json

- Repository context extractor for README and policy files

## Limitations

- The CodeT5 analyzer currently only processes Python files; other languages may not be covered.

- SCA is heuristic-based and does not perform CVE lookups or transitive analysis.

- This automated report is intended as a starting point; manual review is recommended for high-severity findings.

-- End of report (generated locally) --